UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

42640 7590 12/24/2008
DILLON & YUDELL LLP
8911 NORTH CAPITAL OF TEXAS HWY
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/651,548	**Applicant(s)** ATKINS ET AL.	
	Examiner KYUNG Hye SHIN	**Art Unit** 2443	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims **1 - 24** are pending. Claim **17** has been amended. Independent claims are **1, 9, 17**. This application was filed on 8-29-2000.

Response to Arguments

2. Applicant's arguments filed **9-4-2008** have been fully considered but they were not persuasive.

2.1 Applicant argues that the referenced prior art does not disclose, "the associated key comprises a private key. (Remarks Page 8)

Applicant amended the claim limitation to use a private key for the encryption process. Doonan discloses that the associated key is encrypted using a public key. But, Doonan also discloses in a different procedure that a private key within a public/private key pair can be used to encrypt information such as a message or a key. (Doonan col 5, ll 48-50: encrypted with a private key corresponding to digital certificate (private key used for information encryption; implies public key used for decryption)) This encryption process is equivalent to Applicant's claimed limitation of an encryption process. A private key can also be used to encrypt data or information. Doonan discloses a private key can also be used as an associated key.

2.2 Applicant argues that the referenced prior art does not disclose, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system. (Remarks Page 9)

The claimed invention discloses how to enable, “preventing validation of the association of the user with messages”. The action to prevent this is: “by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key”. The association key is deleted (erased) or revoked (revoked definition: see Spec. Page 15 ll 27-28 “Associated key A may be **revoked by simply erasing it** from server system 104.”) as per specification by software component at the user system software component (data encryption system). The specification discloses the procedure which can be used to revoke an associated key. And, Cook discloses this equivalent particular procedure (erasure of key) in order to revoke an associated key.

The claimed invention does not address the fact that “the simple deletion at the sender (i.e., encrypting) system of a message recipient's public key” does not "prevent validation of the association of the user with messages" and does not render the encrypting data processing system unable "to decrypt the encrypted user key” This argued claim limitation and statement is not addressed in the claimed invention. (Remarks Page 10, ll 18-21) The claimed limitation states the procedure to complete (revoke the key) in order to prevent validation of the association of the user with messages.

2.3 Applicant argues the dependent claims. (Remarks Page 10)

Arguments for dependent claims are based upon above arguments for independent claims 1, 9, 17. The successful responses to arguments for independent claims 1, 9, 17, also successfully respond to the current arguments against their respective dependent claims.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. The claimed invention is directed to non-statutory subject matter. Claims **17 - 24** are directed towards a computer program product.

The Specification discloses on page 17, line 34 to Page 18, line 10 that:

> "Programs defining the functions of the present invention can be **delivered** to a data processing system via a variety of **signal-bearing media**, which include, without limitation, non-rewritable storage media (e.g., CD-ROM), rewritable storage media (e.g., a floppy diskette or hard disk drive), and **communication media**, such as digital and **analog networks**. It should be understood, therefore, that such signal-bearing media, when **carrying** or encoding **computer readable instructions** that direct the functions of the present invention, represent alternative embodiments of the present invention."

The disclosure by the specification indicates that, Computer program production instructions can be carried by a signal-bearing media such as a non-rewriteable storage media or a communications media.

Applicant has amended claim language to indicate a computer readable storage medium for carrying the computer readable instructions. But, there is no indication that the computer readable medium is in a state of execution and therefore is directed towards non-statutory subject matter.

Appropriate correction required.

Claim Rejection – 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1 - 4, 6 - 12, 14 - 20, 22 - 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doonan et al.** (US Patent No. **6,807,277**) in view of **Cook** (US Patent No. **6,732,101**).

Regarding Claims 1, 9, 17, Doonan discloses a network messaging system. (Doonan col 1, ll 10-12: *" … present invention is directed to a secure electronic messaging system … "*) Doonan discloses a method, a system and program product for managing a user key used to sign a message for a data processing system, the method comprising:

a) assigning a user key to a user and storing the user key in an encrypted data processing system utilized to encrypt messages; (Doonan col 2, ll 1-7: encryption key assigned by key server for message encryption)

b) encrypting the messages with the user key; (Doonan col 2, ll 7-8: message is encrypted)

c) storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein the associated key comprises a private key; (Doonan col 5, ll 63-67: generate an encrypted user key for transmission; col 5, ll 48-50: additionally; encrypted with a private key corresponding to digital certificate (private key used for information encryption; implies public key used for decryption)))

d) the encrypting data processing system communicating at least one encrypted messages together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; (Doonan col 6, l 1: encrypted message and encrypted key are transmitted to recipient)

f) a computer usable storage medium storing the control program. (Doonan col 3, ll 9-12; col 9, ll 33-44: software exists on computer readable medium for program execution)

Doonan discloses a check on the validation of a sender's credentials. (Doonan col 5, ll 16-20: sender credentials are verified) Doonan does not explicitly disclose revoking the associated key at the encrypting data processing system to prevent validation.

However, Cook discloses:

e) preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key. (Cook col 6, ll 40-50: association key deleted (revoked: see spec. page 15 lines 27-28: "Associated key A may be **revoked by simply erasing it** from server system

104.") as per specification by software component at the user system software component residing (data encryption system))

The specification discloses the procedure to prevent validation of the association key such as by revoking an associated key. Cook discloses an equivalent procedure for revoking or erasing or deleing the associated key.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to delete (revoke) an association key and prevent validation of the association of the user as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38: " *… Messages can be encrypted using any available encryption means at the sender and sent to a forwarding service. The forwarding service can forward the message to each recipient according to the recipient's decryption capability and preference. …* ")

Regarding Claims 2, 10, 18, Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (Doonan col 6, ll 1-3: encrypted key is decrypted)
b) decrypting the messages with the user key. (Doonan col 6, ll 1-3: encrypted message is decrypted)

Regarding Claims 3, 11, 19, Doonan discloses the method, system and program product according to Claims 1, 9, 17, wherein: the encrypting data processing system further comprises a client system and a server system coupled for communication, the client system (Doonan col 3, ll 9-12: network connected client (sender) and server system) having a client memory device and the server system having an encryption chip and a server memory device:

a) storing the user key further comprises storing the user key in the client memory device; (Doonan col 9, ll 44-47: memory area used for data and workspace storage)

b) storing the associated key further comprises storing the associated key in the server memory device; (Doonan col 5, ll 4-5: key is stored at server system database)

Doonan discloses a check on the validation of a sender's credentials. (Doonan col 5, ll 16-20: sender credentials are verified) Doonan does not explicitly disclose preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

However, Cook discloses:

c) preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device. (Cook col 6, ll 40-50: deletion (revocation) of association key at system via software component on server system in order to prevent validation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to prevent validation of messages associated with the user by eliminating the associated key as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38)

Regarding Claims 4, 12, 20, Doonan does not explicitly disclose a server system to receive, encryption and forward message. However, Cook discloses the method, system and program product according to Claims 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server system; (Cook col 2, ll 19-23: send message from client to server for encryption)
b) encrypting the messages using the encryption chip of the server system; (Cook col 2, ll 51-55: encrypt message)
c) sending the encrypted messages from the server system to the client system. (Cook col 2, ll 51-55: deliver encrypted message to recipient (client) system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to send messages, encrypt messages, and retrieve encrypted messages as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38)

Regarding Claims 6, 14, 22, Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising: encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system. (Doonan col 2, ll 3-8: encryption key transferred to sender system)

Regarding Claims 7, 15, 23, Doonan discloses the method, system and program product according to Claims 6, 14, 22, further comprising:
communicating an encrypted associated key to validate the association of the user with the encrypted messages. (Doonan col 5, ll 63-67)

Regarding Claims 8, 16, 24, Doonan discloses the method, system and program product according to Claims 7, 15, 23, further comprising: decrypting the associated key with the encryption chip key. (Doonan col 6, ll 1-3)

7. **Claims 5, 13, 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doonan-Cook** and further in view of **Marshall** (US Patent No. **4,888,800**).

Regarding Claims 5, 13, 21, Doonan-Cook does not explicitly disclose the ability to erase key information after processing of an encrypt message. However, Marshall discloses the method, system and program product according to Claims 4, 12, 20, further comprising: erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (Marshall col 2, ll 30-35: key information is erased from system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan-Cook to erase all key related information after message processing maintaining only current information as taught by Marshall. One of ordinary skill in the art would be motivated to employ Marshall in order to enable a flexible and strengthened network key management system. (Marshall col 1, ll 50-58: " *… system has the advantage … only to maintain the keys required for whatever current communication sessions … a pair of session keys … every time a link or session is requested …* ")

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KYUNG Hye SHIN whose telephone number is (571)272-3920. The examiner can normally be reached on 9:30 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia L. Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kyung Hye Shin
Examiner
Art Unit 2443

KHS
December 15, 2008

/Tonia LM Dollinger/

Supervisory Patent Examiner, Art Unit 2443